AU/ACSC/Kuriatnyk/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

New Tools for Cyber Terrorism

By

Alex N. Kuriatnyk, LCDR, USN

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Lee Hester

Maxwell Air Force Base, Alabama

December 2010

ELA Research Paper
11-4916

New tools used by terrorist organizations are not what we think. Yes, they still have their mortars, IED's, VBIED's and humans sacrifices to explode in some populated area of a country but the tools discussed in this paper are not new at all, but increasing in the terrorists networks. The weapon of choice in the future used by terrorists is called cyber terrorism. The terrorists have been using the internet for more than a decade for its own purposes to further their causes. However, they haven't used it as a weapon yet, but we would be naïve to think that will not change. The terrorists are using more sophisticated technologies in the cyber realm and with their financial clout they could take down or disrupt our critical infrastructure or use a cyber attack as a secondary attack to a primary massive kinetic strike because the US has underestimated the cyber criminal and cyber terrorist.

Since the early nineties terrorist organizations have been using the internet for communications purposes. In particular, during the Israel and Palestinian conflict the HAMAS was known to deface the Israeli web sites and vice versa. The terrorist group al Qaeda has used the internet to share best practices and lessons learned with other militant groups. They have constantly used the internet to their advantage. During the war with Afghanistan, lap top computers were discovered in a cave that contained aircraft design used in the coordinated attacks on the World Trade Center. They have used the internet as a recruitment tool and communications tool to enlist and train future terrorists. Terrorist cells have been created all over the world to support the al Qaeda cause. They use of the internet and use secret encrypted chat rooms to publish instructions on how to build bombs, techniques, tactics and procedures to carry out future attacks. As stated by the Heritage Lectures in 2009, "The anonymity and difficulty of tracing interactions in restricted, password protected chat rooms and the use of encrypted e-mails give terrorists a much greater degree of operational security"[1]. Terrorists are using our own

technology against us and choosing this type of communications as their primary source. Terrorists are more proficient at using the internet for propaganda and fund raising techniques. In 2003 The Institute for Technological Studies at Dartmouth College stated, "The use of the internet to spread propaganda speaks to the terrorists' and sympathizers' desire to target certain audiences, such as the educated but disenfranchised and the intelligentsia in Islamic countries, and the well educated expatriates residing in the western world."[2] The terrorists have been using the internet for fundraising campaigns to pay for their extensive operations and coordinated attacks. The Islamic terrorists particularly al Qaeda are using cyber technologies to raise money in several different ways. One approach is to move funds through legitimate web sources unbeknownst to the generous honest people but there is evidence they participate in criminal activities as well. "According to testimony by Dennis Lormel (Chief, Terrorist Financial Review Group, FBI) before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information (July 9, 2002), "… an Al-Qaeda terrorist cell in Spain used stolen credit cards in fictitious sales scams and for numerous other purchases for the cell."[3] Al Qaeda made purchases in small amounts so identification was not necessary. There are many other documented accounts of Islamic criminal activities through the use of the internet. The mujahidin have used false passports and travel documents to open up bank accounts to fund their cause. INFOCOM, a computer based company in Dallas, Texas was shut down in 2003 for laundering money for the Hamas. According to the FBI these trends will continue until more resources can be applied to stopping these criminals.

Is there a possibility that al-Qaeda can carry out an attack on the US infrastructure? There are many views on this subject, some say it would not provide the necessary shock and awe that al-Qaeda wants to promote. Others say al-Qaeda does not possess the resources nor the

capabilities to carry out a sustained attack on US infrastructure. Others say it's inevitable and we should prepare.

Mr. Lewis in 2002 from the Center of Strategic & International Studies argues that we have to put cyber terrorism into context. "His definition of cyber terrorism is the use of network computer tools to shut down critical national infrastructure (such as energy, transportation or government operations) or to coerce or intimidate the government or population."[4] He proposes to set a threshold on an attack and if that threshold is not met than the attack is insignificant. He also suggests that we have energy and, transportations outages all of the time and we are prepared for minor outages or disruptions. He states, "It is particularly important to consider that in the larger context of economic activity, water system failures, power outages, air traffic disruptions and other cyber-terror scenarios are routine events that do not affect national security."[5] He further goes on to state "For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers, terrorist groups or nation states…"[6] Even though Mr. Lewis makes and compelling argument there are others who do not share is opinion.

In early as 2001, Condoleezza Rice said, "Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation." In 2005 the US Army released its TRADOC manual titled Cyber Operations and Cyber Terrorism and they take a different point of view than Mr. Lewis. In the manual it states that US infrastructure is a prime candidate for the terrorists to attack. The electrical power grids as well as all other US infrastructure is controlled by supervisory control and data acquisition (SCADA) systems to include a host of computer related equipment that regulate the flow and amount of water, emergency service systems or electricity via the internet. The TRADOC manual also states, "If unauthorized personnel gain cyber access to these systems, any alterations to settings or data can have disastrous consequences similar to

physical sabotage..."[7] The effects of these possible disruptions could also affect the military by disrupting transportation and C2 operations.

There are several reports of criminals hacking into the SCADA systems causing private companies to pay the ransom because it was less costly than the alternative of being shut down. Heritage Lectures stated in 2009, "A lucrative target is data well beyond personal identity and financial information. Infiltrating businesses and stealing industrial secrets, pharmaceutical formulas, and like data can reap huge profits for criminals"[8]. If cyber criminals are capable of these crimes imagine if Bin Laden could hire these perpetrators. The possibility of these hired guns be part of a coordinated cyber kinetic attack with biologic, chemical, or nuclear weapon and simultaneously use a cyber attack preventing emergency responders to react. These hired guns would be easy to convince of such an operation since it's always about the money for them.

Some of the new tools that cyber terrorists could use are easily accessible and most if not all are available on line for purchase. These tools when purchased would come with instructions for constructing and deploying a virus or a series of viruses to cause devastating affects to our cyber realm. There are a host of tools that can be used by the cyber terrorist to include back door (a way in to a system), Denial of Service (DOS) is designed to disrupt networks, key loggers, Trojan horse, logic bombs, worms and zombies. All of these tools have been identified by the 2005 DCINST Handbook 1.02 "Cyber Operations and Cyber terrorism". Another potential tool is the botnet, relatively a new tool that gives the criminal the ability to launch a group of computers in the range of 100,000 or more without the owner's knowledge. These botnet's are used in phishing scams, distributed denial of service (DDOS) and when used costs the government millions of dollars. According to the 2009 criminology report by McAfee, they state, "… anyone can go to a criminal group and rent a botnet. We've reached a point where you only

need money to cause disruption, not know-how and this is something that needs to be addressed."[9] Symantec Corp., another computer virus company detected over 62,000 botnet infected computers from July through December, 2007. In 2007 the FBI uncovered a botnet campaign that was worth 20 million dollars. The cost of these botnet interruptions has cost the US government billions of dollars each year. The consequences of these botnets could shut down a network service by sending hundreds of thousands of pings to a specific server bogging it down. These types of attacks would be a prime candidate for a DOD or SCADA attack. There are precautions that the US government can take to lessen the chance of cyber terrorist attacks.

The Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee in March of 2009 recognizes the growing cyber and organized crime threat. According to the report they see the growing array of state and non-state actors targeting the US. It states, "A growing array of state and non state adversaries are increasingly targeting for exploitation and potentially disruption or destruction-our information infrastructure, including the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[10] Over the past year they recognized an increase in cyber exploitation and the potential attacks. It goes on further to state, "Terrorist groups, including al-Qaeda, HAMAS and Hezbollah have expressed the desire to use cyber means to target the United States."[11] In January of 2008, the Comprehensive National Cybersecurity Initiative (CNCI) was adopted as national policy.

The CNCI address current and future cybersecurity threats and technologies and develops a framework to work with civilian agencies to combat cyber criminals and terrorists. The CNCI comprises of education, defensive, offensive, R & D, and COIN elements. One objective of the CNCI is to remain sensitive to the protecting the privacy and rights of US citizens. The CNCI

states, "We are witnessing an unprecedented unity of effort across a broad coalition of government agencies, members of congress, and leaders of industry.[12] The cyber criminal and terrorist have always stayed one step ahead of us, now with the CNIC and the Senate Armed Service Committee threat assessment of March 2009 will put us on a level playing field. Some startling figures in the report suggest it cost our government 42 billion dollars for spam and a cost of 141 billion dollars worldwide in 2008 and it's estimated that global companies have lost 1 trillion dollars worth of intellectual property to data theft. It is quite obvious that if we don't get a handle on cyber criminals it's only a matter of time before the cyber terrorists get their chance.

Terrorist organizations have been and will continue to use the internet for communications, recruitment, financial, propaganda and intelligence. It is only a matter of time before they start using it as an offensive weapon. The terrorist organizations that are most likely attack the US will be al-Qaeda, HAMAS and Hezbollah, since they have vowed to eliminate all western influence in the Islamic world. It could come as major critical infrastructure take down or a prelude to a kinetic attack, but one thing for certain, it will happen. Terrorists will eventually take advantage of the cyber realm for offensive operations and when they realize they need help they will hire cyber criminals. These criminals are sophisticated and highly capable of assisting the terrorists. It has cost the Government 42 billion dollars alone just in spam emails and the world approximately 141 billion in 2008. There are many weapons available to the terrorist in the cyber realm and many of them were mentioned in this paper and easily attained, but in particular the botnet could overload a SCADA system or a DOD computer and render it inoperable for hours or weeks depending on the severity of the attack. The US government must take better precautionary measures to protect our critical infrastructure and business's from these types of attacks. The Government in 2008 has started taking actions to combat cyber criminals

and cyber terrorists. With the establishment of the CNIC and threat assessment by Senate Armed Forces Committee the US Government will be ready and able to combat future attacks on our critical infrastructure and private businesses. There is no certain way to know if we will be able to prevent a cyber terrorist attack but we can make our country better prepared and equipped to lessen the severity when one does actually occur.

[1]www.heritage.org/Research/NationalSecurity/hl1123.cfm , accessed 02 DEC 09

[2] Institute for Security Technology Studies at Dartmouth College, *Examining Cyber Threats in Islamic groups,*Technical Analysis Group, 2003

[3] IBID

[4] Center for Strategic and International Studies *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats***,** James A. Lewis December 2002

[5] IBID, pg 3.

[6] IBID pg 3.

[7] Paul Oman, Edmund Schweitzer, and Jeff Roberts, "Protecting the Grid from Cyber Attack Part I:Recognizing Our Vulnerabilities," *Utility Automation and Engineering T&D*, November 2001; available from http://uaelp.pennnet.com;

[8] www.heritage.org/Research/NationalSecurity/hl1123.cfm , accessed 02 DEC 09

[9] www.mcafee.com, *Virtual Criminology Report 2009,*accessed on 10 DEC 09

[10] SASC at a March2009 DNI Statement for the Record, pg 39.

[11] IBID, pg 40.

[12] IBID, pg 40.